Govern AI Confidently with CDW and Microsoft

As organizations deploy Microsoft 365 Copilot and AI agents, security and governance become foundational. Copilot agents interact with company data, user identities and business systems, meaning they must be deployed with the right controls in place to prevent oversharing, data exposure and compliance risk.

Microsoft Copilot is built on enterprise-grade security, but organizations still need to configure, govern and monitor their environment to ensure AI agents operate safely at scale.

CDW helps organizations put the right guardrails in place so Copilot agents can deliver value securely and responsibly.

Why Securing Copilot Agents Matters

The shift from AI experimentation to production introduces new risks:

- Oversharing of sensitive data
- Inconsistent governance across agents
- Identity and access gaps
- Limited visibility into agent activity and usage

To scale AI safely, organizations need clear governance, strong identity controls and continuous security monitoring.

How CDW Helps Secure Copilot & AI Agents

Microsoft 365 Governance Workshop

Set the right governance from day one. AI agents should follow the same rules as your people and data. CDW works with your team to define governance policies that control how Copilot and AI agents access information, interact with users and operate across Microsoft 365.

What this helps you do:

- Define clear guardrails for Copilot and AI agent usage
- Reduce the risk of oversharing or misuse
- Align AI adoption with your organization's compliance and security standards

Microsoft CDW

Understand and Strengthen Your Security Posture

Microsoft Security Assessment

Before scaling Copilot agents, it's critical to understand how secure your environment really is. CDW evaluates your Microsoft 365 security posture to identify gaps that could impact AI agent security.

What this helps you do:

- Review identity, access and data protection controls
- Identify security gaps that could expose sensitive data
- Ensure Copilot agents operate in a secure, compliant environment

Control Who and What Has Access

Identity & Access Management (IAM) Services

Identity is the first line of defence for AI. CDW helps ensure only the right users and the right AI agents can access sensitive information.

What this helps you do:

- Enforce multifactor authentication and conditional access
- Limit AI agent access to approved data and users
- Reduce the risk of unauthorized or excessive access

Monitor and Respond to Threats

Managed Detection & Response (MDR)

AI agents don't stop working after hours, and neither should security. CDW provides 24/7 monitoring and threat response across your Microsoft security environment to help protect AI activity and sensitive data.

What this helps you do:

- Detect and respond to suspicious activity in real time
- Monitor identity, endpoint, cloud and data threats
- Reduce the impact of security incidents before they escalate

Ensure a Secure Cloud Foundation

Hybrid Cloud Foundation for AI

Most organizations run in hybrid environments, where data and applications span on-premises systems and Microsoft Azure. Copilot agents frequently interact across this landscape, making hybrid cloud governance critical. CDW helps organizations build secure hybrid foundations, so Copilot agents operate safely and at scale.

What this helps you do:

- Enable secure access to data across on-premises and cloud environments
- Apply consistent identity, security and governance controls for Copilot agents
- Support secure, scalable AI adoption in real-world hybrid IT environments

Ready to Secure Your Copilot Agents?

CDW helps you adopt AI responsibly so your teams can innovate faster without compromising security.

Talk to your CDW Account Manager or give us a call at **800.972.3922**

Microsoft CDW